IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Graeme John Proudler et al.	) On Appeal to the
	) Board of Appeals
Patent Application No.: 09/913,452	)
	) Group Art Unit: 2825
Filed: 12/05/2001	)
	) Examiner: Do, Thuan V
	)
For: " Trusted Computing Platform"	) Date: April 28, 2005

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal from the Final Rejection, dated November 2, 2004, for the above identified patent application. The Applicants submit that this Appeal Brief is being timely filed, since the Notice of Appeal was filed on March 1, 2005 and this Appeal Brief is accompanied by a request for a one month extension of the term.

REAL PARTY IN INTEREST

The present application has been assigned to Hewlett-Packard Development Company of Houston, Texas.

STATUS OF CLAIMS

Claims 1-10, 12-17 and 22-52 are currently pending and are reproduced in the accompanying appendix. Claims 1-10, 12-17 and 22-52 are the subject of this Appeal. The Examiner has allowed none of the claims. The Examiner also objects to claim 54 as allegedly being unclear.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

OPENING STATMENT

The prosecution of this application has been a very frustrating experience for the Applicant, the assignee and the undersigned. As the Board of Appeals will see as it works its way through this Brief, the Applicants have been kept in the dark with respect to the Examiner's rationale for rejecting many of the claims. When pressed[1] into engaging in a telephone interview with applicants' attorney, the Examiner avoided discussing why many of the claims have been rejected or told applicants' attorney effectively that the Examiner "must have had some reason for rejecting the claim" and therefore "the anticipatory material must be in the reference someplace." That is, of course, a gross violation by the Examiner of the rules of practice. See 37 CFR 1.104(c)(2) which requires the Examiner to designate in complex references "the particular part relied upon…as nearly as practicable." Since the cited reference (Ginter et al) is over 400 pages long, the Examiner's actions are simply improper.

So, in the case of the rejections of some of the independent and many of the dependent claims, the Applicants have no idea what portion or portions of the cited reference is/are allegedly pertinent thereto. However, as will be seen, it is the Applicants' position that the cited art is largely irrelevant to even the independent claims on appeal and therefore it is perhaps not too surprising that it does not even come close to anticipating the dependent claims. What utterly amazes the Applicants is that the Examiner stands on a final rejection while at the same time cannot tell the Applicants why most of the claims are being rejected.

---

[1] The latest interview with the Examiner was only granted after the undersigned telephoned the Examiner's supervisor to complain that his official actions were incomplete and that the applicant would bring these deficiencies to the Attention of the Board of Appeals if the Examiner refused to make his rejections clear. So the Examiner begrudgingly granted an interview request, but at the same time severely limited the number of issues which could be discussed and terminated the interview prematurely when asked to identify the portions of the prior art reference he is relying upon in making the present rejections.

SUMMARY OF INVENTION

Computers are subject to tampering, and such tampering can compromise a formerly acceptable or secure computing platform rendering it unacceptable instead. The invention described and claimed in the present application relates to a trusted computing platform which has features allowing a user or other manager to detect that it has been compromised.

The nature of the compromise can be, for example, the removal of an original BIOS chip and its replacement by a rogue BIOS chip which is designed to send data to some 'undesirable' location when the computer is used. The present invention can be used to identify the presence of a rogue BIOS chip, for example, by acquiring a true value of an integrity metric of the computer system, preferably before the computer system is booted.

Overview of independent Claims

Claim 1 is an apparatus claim which recites a number of computer apparatus limitations in combination with "a trusted device" each being connected for communication with one or more other components wherein the trusted device is "arranged to acquire a true value of an integrity metric of the computing apparatus."

Claim 22 is somewhat similar to claim 1, but in this claim the trusted device is recited as being "adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric."

Claim 12 is a method claim which recites a "method of operating a system comprising a trusted computing apparatus and a user, the trusted computing apparatus incorporating a trusted device being arranged to acquire the true value of an integrity metric of the trusted computing apparatus, the method comprising the steps of:

the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus;

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party."

Claim 35 recites, in "a computing apparatus comprising an assembly, a plurality of functional components including a main memory and a main processor mounted on the assembly, each functional component being connected for communication with one or more other functional components on the assembly, a trusted device being one of said functional components and adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric."

Claim 36 recites a "trusted device for use as a functional component in a computing apparatus, the trusted device being adapted for mounting on an assembly of the computing apparatus and being adapted for communication with other functional components of the computing apparatus, the trusted device being adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric."

Each of the independent claims includes a recitation of a "trusted device" which either acquires "a true value of an integrity metric of the [trusted] computing apparatus" (see claims 1 and 12) or acquires "a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric" (see claims 22, 35 and 36).

Overview of dependent Claims

This application includes a number of dependent claims which present additional features and/or aspects of the inventions of the independent claims.

Some of the dependent claims describe the "trusted device" in greater detail or describe its relationship to other elements of the claims. See for example, dependent claims 2-6, 25-30, 37-39 and 44, 47-49, and 53.

Some dependent claims recite operations performed on particular data stored in the trusted device. See, for example, claims 7-9, 31-33, and 40-42.

Some claims are more or less combinations of the foregoing. See, e.g., claim 10 and 54.

Other dependent claims recite or refer to a challenge and its possible features, including a nonce and/or encryption, and/or the response to the challenge. See, e.g., claims 13 - 15, 34, and 43.

While still other claims relate to the nature of the integrity metric and/or when it is determined. See, for example, claims 23, 24 and 45-46, and 49-53.

ISSUES

Issue 1: Are Claims 1-10, 12-17 and 22-52 patentable under 35 USC 102 over the cited art?

Issue 2: Is claim 54 sufficiently clear to avoid an objection by the Examiner?

Issue 3: Is a rejection under 35 USC 102 proper just because a claim is allegedly similar to another claim in the same patent application?

Issue 4: What is the applicant's remedy when the Examiner violates the Rules of Practice?

GROUPING OF CLAIMS

For each ground of rejection which the Applicants contest herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together.

THE ARGUMENT

Issue 1: Are Claims 1-10, 12-17 and 22-52 are patentable under 35 USC 102?

In the Office Action of July 15, 2004, the Examiner finally rejects Claims 1-10, 12-17 and 22-52 as being fully anticipated by US Patent No. 5,892,900 to Ginter et al. Applicants respectfully disagree with the conclusions that the Examiner has made with regard to the teaching of Ginter et al (hereinafter "Ginter") and submit that Ginter does not teach, disclose or suggest all of the claim limitations of the rejected claims.

Now the rejection of the specific claims by the Examiner based on the disclosure of Ginter et al will be addressed.

Claim 1

Claim 1 is set forth in the enclosure. The limitation at issue in claim 1 includes the recitation: "the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus.

In rejecting claim 1 under 35 USC 102, the Examiner points to a rather short passage in Ginter at column 68, lines 29-42.

Before discussing the specific passage pointed to by the Examiner, it is useful to note that Ginter is a very long patent, including over 400 pages of drawings and type set specification. Ginter is concerned with systems and methods for secure transaction

management and electronic rights protection. Ginter is concerned with financial or electron commerce transactions (for example) occurring on the "information highway" (see col 1, lines 41-49) and securing those transactions (see col 2, lines 8-17). So Ginter proposes what he calls a "virtual distribution environment" or simply "VDE" that secures, administers and audits electronic information use. (See col 2, lines 20-32).

Ginter tells the reader that a software solution (see col 6, lines 30-56) is disclosed which addresses many issues associated with electronic commerce.

Ginter also tells the reader about the hardware which VDE runs on. Ginter initially tells the reader that VDE can run on anything between "an inexpensive hand-held device to large mainframe computers." (see col 4, lines 59-61).

However, Ginter also includes a discussion of Secure Processing Units or SPUs which apparently can be used to "achieve the electronic contract/rights protection environment" of Ginter's invention.

The Examiner focuses on Ginter's SPU, but one needs to appreciate the context in which Ginter tells his story about his invention. Ginter is primarily concerned about the security of electronic commerce transactions. So much so that Ginter suggests utilizing specialized hardware to meet those ends. His specialized hardware helps ensure the security of electronic commerce.

Ginter shows some concern for the physical security of the computers upon which his software runs. He makes certain suggestions, such as using a tamper resistant barrier 502 (see figure 6). Ginter informs the reader that:

> "Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources,

processes and information within SPU 500. In one example, **tamper resistant security barrier 502 is formed by security features** such as "encryption," and **hardware that detects tampering** and/or destroys sensitive information within secure environment 503 when tampering is detected." [Emphasis added] (Col 60, lines 17-28).

Ginter tells the reader more about his tamper resistance barrier 502 a few pages later in his patent where the reader is informed:

"As shown in FIGS. 6 and 9, SPU 500 may be surrounded by a tamper-resistant hardware security barrier 502. Part of this security barrier 502 is formed by a plastic or other package in which an SPU "die" is encased. Because the processing occurring within, and information stored by, SPU 500 are not easily accessible to the outside world, they are relatively secure from unauthorized access and tampering. All signals cross barrier 502 through a secure, controlled path provided by BIU 530 that restricts the outside world's access to the internal components within SPU 500. This secure, controlled path resists attempts from the outside world to access secret information and resources within SPU 500."

"It is possible to remove the plastic package of an IC chip and gain access to the "die." It is also possible to analyze and "reverse engineer" the "die" itself (e.g., using various types of logic analyzers and microprobes to collect and analyze signals on the die while the circuitry is operating, using acid etching or other techniques to remove semiconductor layers to expose other layers, viewing and photographing the die using an electron microscope, etc.) ..."

"To increase the security of security barrier 502 even further, it is possible to encase or include SPU 500 in one or more further physical enclosures such as, for example: epoxy or other "potting compound"; further module enclosures including additional self-destruct, self-disabling or other features activated when tampering is detected; further modules providing additional security protections

> such as requiring password or other authentication to operate; and the like. In addition, further layers of metal may be added to the die to complicate acid etching, micro probing, and the like; circuitry designed to "zeroize" memory may be included as an aspect of self-destruct processes..."

So, from Ginter's (and the reader's) perspective, the important things in terms of physical security are (i) using a tamper resistant barrier and (ii) making your chips less susceptible to reverse engineering.

So, now let us turn to the Examiner's rejection of claim 1. The Examiner points to a pattern matching engine 524 that is inside SPU 500 mentioned above. The passage cited by the Examiner is not that long, so it is reproduced below:

> Optional pattern matching engine 524 may provide special purpose hardware for performing pattern matching functions. One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way. In addition, certain forms of usage (such as logical and/or physical (contiguous) relatedness of accessed elements) may require searching potentially long strings of data for certain bit patterns or other significant pattern related **metrics**. Although pattern matching can be performed by SPU microprocessor 520 under software control, providing special purpose hardware pattern matching engine 524 may speed up the pattern matching process. [emphasis added] (Col 68, lines 29-42).

Ginter's reference to VDE objects in the above paragraph appears to be nothing more than a reference to a data object or structure. See Figure 5A and the related description. Note also the use of the word "metric" (in its plural form) in Ginter. This is the only passage in Ginter that the word "metric" appears. The word also appears in each of the independent claims pending in this application.

It is the Applicants' belief that the Examiner did a search for the word "metric", found it in Ginter and since Ginter is a very long disclosure (which seems to almost include the proverbial kitchen sink), the claims were rejected more of less on that basis. Of course, the mere presence of the word "metric" (in its plural form) in Ginter does not anticipate claim 1.

In order to properly reject a claim under 35 USC 102, the Examiner has the burden of showing where each and every limitation of each and every rejected claim is disclosed by a prior art reference.

Claim 1 recites, *inter alia*, "the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus."

In terms what apparatus in Ginter allegedly meets the trusted device limitation and what allegedly meets the "true value of an integrity metric of the computing apparatus" limitation, the final rejection is **vague** on the first point and **silent** on the second point.

Has the Examiner met his burden of proof in rejecting claim 1? No, indeed not!

Perhaps, based on the cited passage, the Examiner contends that Ginter's pattern matching engine 524 meets the "trusted device" limitation of claim 1. One might then wonder what Ginter's pattern matching engine 524 is for. Apparently it is supposed to help check in "comparing long data strings to determine whether they compare in a predetermined way" and these data strings apparently relate to somehow authenticating Ginter's VDE Objects 300, that is, his software structures. Anyway the search which is optionally done in Ginter by element 524 is a search for "certain bit patterns or other significant pattern related metrics" (whatever those pattern related metrics might be). Even though Ginter is unclear on the specifics, it seems clear that Ginter is suggesting that incoming electronic commerce data can be searched for certain patterns or other significant pattern related metrics. Ginter is equally clear that these metrics are quite

unrelated to the integrity of his hardware environment, the protection of which he discusses a few pages earlier (as discussed in the passages first reproduced above).

Ginter's pattern matching engine 524 is associated with Ginter's SPU 500 and therefore it is located inside barrier 502 (see Figure 9A). It is one of the items meant to be protected by barrier 502 and not something which acts as a "trusted device" "arranged to acquire a true value of an integrity metric of the computing apparatus" as claimed by claim 1.

When these deficiencies were pointed out in the aforementioned telephone call with the Examiner after the final rejection issued, the Examiner then tried to justify his rejection of claim 1 asserting that SPU 500 (instead of element 524 discussed in the passage cited in the final rejection) meets the "trusted device" limitation. The Examiner was asked how the SPU 500 allegedly meets the limitation quoted above about the trusted device (now SPU 500) being "arranged to acquire a true value of an integrity metric of the computing apparatus". The Examiner could not supply a reasonable answer and stated if the applicant disagreed with the position he was taking that the applicant's remedy was to file an appeal.

Claim 1 is not anticipated by Ginter. The metrics in Ginter to which the Examiner refers relate only to data pattern matching and not to the "integrity" "of the computing apparatus" as claimed by claim 1. Additionally, how does Ginter's "metric" supposedly meet the "acquire a true value" limitation of claim 1 wherein claim 1 recites that "the trusted device" is "arranged to acquire a true value of an integrity metric"? How is Ginter's metric acquired and what assures that it is a "true value" of anything, much less "of the computing apparatus" as claimed by claim 1? The final rejection is silent. The rejection of claim 1 is improper and should be reversed by this Board of Appeals.

Claim 2

Claim 2 adds the limitation "the trusted device comprises device memory means and means for instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means" to the limitations of claim 1.

The final rejection is silent on where this limitation is allegedly met by Ginter. As such the final rejection is clearly defective and should be reversed.

Of course, the Examiner could surely point to memory devices and processors in Ginter, but claim 2 is specific in indicating that the trusted device includes the recited elements. So if element 524 allegedly meets the trusted device limitation as apparently asserted in the final rejection, how is this limitation of adding additional elements allegedly met by element 524?

Also, the Examiner's stated grounds for finally rejecting claim 2 is merely because it is allegedly "similar" to claim 1. That is not a proper basis for rejecting a claim under 35 USC 102 as 35 USC 102 imposes no such requirement on the claims submitted by Applicants.

Claim 3

Claim 3 adds the limitation "the means for instructing the main processing means comprises, stored in the device memory means, program code native to the main processing means, and the trusted device is arranged to transfer the instructions of the program code to the main processing means" to the limitations of claims 1 and 2.

In the final rejection the Examiner points to col 78, lines 56-67 of Ginter as meeting this limitation on page 4 of the final rejection.

Since the Examiner points to element 524 in the final rejection as meeting the "trusted device" limitation, the passage cited by the Examiner is quite irrelevant. If the Examiner switches horses and instead points to SPU 500 as meeting the "trusted device" then what meets the "main processing means" limitation of claim 2 or the limitation of claim 3 that the trusted device "is arranged to transfer the instructions of the program code to the main processing means"? This claim also requires the instructions of the program code in question to "determine the integrity metric" (recited by claim 2) and wherein the integrity metric is an "integrity metric of the computing apparatus" (as recited in claim 1). Where is there any disclosure of any such code in Ginter? Note the cooperation between the claimed trusted device and the claimed main processing means. There is plenty of VDE code in Ginter, but what about the claimed code or the claimed cooperation between the trusted device and the main processing means? Since the Examiner has not pointed either to anticipatory code or such cooperation, the rejection must fail.

Also the Examiner's stated grounds for finally rejecting this claim is merely because it is allegedly "similar" to claim 1. That is not a proper basis for rejecting a claim under 35 USC 102 as 35 USC 102 imposes no such requirement on applicant.

Claim 4

Claim 4 adds the limitation "wherein the computing apparatus is arranged to cause the instructions to be the first instructions executed after release from reset" to the limitations of claims 1-3.

In the final rejection the Examiner points to col 79, lines 35-40 of Ginter as meeting this limitation on page 4 of the final rejection.

Since the Examiner points to element 524 in the final rejection as meeting the "trusted device" limitation, the passage cited by the Examiner is quite irrelevant. If the Examiner switches horses and instead points to SPU 500 as meeting the "trusted device" then it should be noted that the "the instructions to be the first instructions executed after release from reset" (recited by claim 4) are the instructions referred to in the preceding claims, namely, the instructions which "determine the integrity metric" (recited by claim 2) and wherein the integrity metric is an "integrity metric of the computing apparatus" (as recited in claim 1). The Examiner's analysis basically ignores these limitations.

Ordinarily, the first instructions which a processor executes after release from reset are the instructions in its BIOS chip. Is Ginter really any different in that regard? Does the passage cited by the examiner suggest a different way of acting when resetting Ginter's computer? According to Ginter the instructions after reset are fetched from SPU memory 532, and since SPU memory 532 includes a ROM (see Figure 9), a person skilled in the art is lead to understand that the reboot occurs normally based on the contents of the ROM and there is certainly no suggestion in the passage noted by the Examiner that the first instructions after reset "determine the integrity metric" (recited by claim 2) and wherein the integrity metric is an "integrity metric of the computing apparatus" (as recited in claim 1). Ginter teaches that confidence for a secure system can properly rest in his SPU. The present application teaches that such confidence is misplaced. So the host processor (the main processing means of claim 3) is guided by the trusted device to acquire a true value of the integrity metric of the computing apparatus (claim 1) using instructions of the program code transferred from the trusted device to the main processing means (claim 3) which instructions are the first instructions processed after release from reset (claim 4).

One of the features of applicant's invention of claim 4 is that you can detect whether or not a rogue BIOS chip has been installed in a compromised computer before any instructions in the rogue BIOS chip are executed. Ginter does not hint at any such solution or even recognize the problem in the passage cited by the Examiner.

Also the Examiner's stated grounds for finally rejecting this claim is merely because it is allegedly "similar" to claim 1. That is not a proper basis for rejecting a claim under 35 USC 102 as 35 USC 102 imposes no such requirement on Applicants' claims.

Claim 5

Claim 5 adds the limitation "where the trusted device is arranged to transfer the instructions to the main processing means in response to memory read signals from the main processing means."

In the final rejection, the Examiner is basically silent on why claim 5 is being rejected.

If the claimed "trusted device" corresponds to element 524 of Ginter, then how does that element possibly meet the limitations quoted above? If, on the other hand, the Examiner is now asserting that Ginter's SPU 500 meets the claimed "trusted device" limitation, how is Ginter's SPU "arranged to transfer the instructions to the main processing means (whatever that is) in response to memory read signals from the main processing means"?

The Examiner has not provided a proper statutory basis for rejecting this claim under 35 U.S.C. 102 and therefore the rejection should be overturned.

Claim 6

Claim 6 adds the feature "wherein the trusted device comprises device memory means and is arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device."

The final rejection made by the Examiner is basically silent on why this claim is being rejected. On what elements in Ginter does the Examiner believe that "a data bus means" or "a flag" read? Where, for example, is there any disclosure of the setting or storage of a "flag in the event that the first memory read signal is generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device"?

Since the Examiner has not pointed out how that claim is allegedly anticipated by the cited reference, the rejection must fail.

Moreover, Applicant should not have to speculate where in a 400-page reference there might be something that the Examiner considers to be the equivalent of a flag. Perhaps the Examiner has not even considered this issue. The Rules of Practice make it clear that the onus is upon the Examiner to make clear the grounds for rejection. See 37 CFR 1.104(c)(2). The Examiner's disregard for the rules of practice is very troublesome for Applicants.

Claim 7

Claim 7 adds the recitation, to claim 1, "wherein the trusted device has stored in device memory means at least one of: a unique identity of the trusted device; an authenticated integrity metric generated by a trusted party; and a secret."

Again, the Applicant is told in the final rejection that the only reason that this claim is being rejected is that it is "similar" to claim 1.

In the aforementioned telephone call with the Examiner, the undersigned asked the Examiner where the limitation "a unique identity of the trusted device" found in claim 7 is disclosed is Ginter. The Examiner responded with something pretty close to " I must have had something in mind when I rejected the claim, but unfortunately now I cannot think of what I had in mind." Well, that sort of rejection just does not comport with 37 CFR 1.104(c)(2).

Anyway, the Examiner apparently admits that while he may have had something in mind when rejecting the claim, but apparently does not feel the need to inform the Applicants of what his reasoning might be when he make the rejection final. This is improper.

Since the Examiner has not met the statutory burden for rejecting a claim under 35 USC 102, nor has the Examiner complied with the Rules of Practice in rejecting this claim, the rejection should be properly reversed by this Board of Appeals.

Claim 8

Claim 8 adds to claim 7 the limitation "wherein the trusted device has stored in device memory means a secret comprising a private asymmetric encryption key."

In the telephone conversation with the Examiner alluded to above, the undersigned asked the Examiner what he was reading the "secret" limitation of claim 8 upon and, moreover, what he was reading the limitation of "a private asymmetric encryption key" in Ginter. The Examiner could not or would not tell the undersigned what portions of the Ginter reference the Examiner is relying upon to reject claim 8.

Since the Examiner has not met the statutory burden for rejecting a claim under 35 USC 102, nor has the Examiner complied with the Rules of Practice in rejecting this claim, the rejection should be properly reversed by this Board of Appeals.

Claim 9

Claim 9 adds the limitation "wherein the trusted device also has stored in device memory means a respective public encryption key that has been signed by a trusted party."

Again, the final rejection is silent on why this claim is being rejected.

Since the Examiner could not advise the undersigned, in the telephone conversation alluded to above, why the claim upon which this claim is dependent, was rejected, it seemed to the undersigned that it would be a futile act to ask the Examiner why claim 9 was being rejected. In any event, the Examiner concluded the interview and refused to discuss the rejections of most of the claims pending in this application even though the final rejection is silent as to why they are being rejected.

Since the Examiner has not met the statutory basis for rejecting claim 9 under 35 USC 102, nor has the Examiner complied with the Rules of Practice, this grounds for rejection should be properly reversed by this Board of Appeals.

Claim 10

Claim 10 adds the recitation to claim 8 that "wherein the trusted device has stored in device memory means an authenticated integrity metric generated by a trusted party and includes an encryption function, the trusted device being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key."

Unfortunately, the final rejection sheds no light as to why this claim is being rejected.

Since the Examiner has not demonstrated why each and every limitation of claim 10 is anticipated by Ginter, this rejection must fail. In the telephone conversation with the Examiner alluded to above, we did not even go all the way through claim 10 before the Examiner decided to conclude the interview. The undersigned asked the Examiner what he was reading "an authenticated integrity metric" upon and what the "trusted party" was in terms of his rejection of the claim based upon Ginter. The Examiner was either unable or unwilling to advise the undersigned of just what basis he is rejecting claim 10 upon. About the only thing the Examiner was able to point to was that Ginter talks about an encryption function at column 8, beginning at

line 1. At that point, Ginter talks about using cryptographic techniques and other technologies with his VDE approach to electronic commerce. Since Ginter does not meet the limitation "the response comprising an acquired integrity metric and the authenticated integrity metric", the fact that Ginter has some sort of encryption technology associated with it does not mean that the limitation "both signed by the encryption function using the private asymmetric encryption key" is anticipated by Ginter.

Moreover, note in claim 10 that this claim also recites that "the trusted device" is "arranged to generate a response to a received challenge." Where does Ginter teach that? Since the Examiner has not deigned to advise either the applicant or this Board how claim 10 is allegedly fully anticipated by Ginter, the Examiner's rejection of Ginter based upon 35 USC 102 must be overturned.

Claim 12

Claim 12 is another independent claim in this application that recites a method of operating a system comprising a number of elements. Instead of reciting the claim in its entirety here, the Board is directed to the enclosure wherein the claim can be found.

The Examiner rejects claim 12 on pages 2 and 3 of the final rejection, the Examiner again pointing to element 524 of Ginter in making the rejection.

Apparently, it would be the intention of the Examiner to again cite Ginter, column 68, lines 29-42, wherein the word "metric" can be found (in its plural form). However, other than that, that passage is irrelevant to claim 12 since there is certainly no disclosure of a "integrity metric" of the entrusted computing apparatus" as specifically claimed by claim 12.

Claim 12 also recites "generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus..." The Examiner recites column 68, lines 29-42 of Ginter. Again, this is merely the passage noted above with

respect to the pattern generating engine 524 of Ginter. Since the Applicants cannot see anything vaguely resembling "generating a challenge for the trusted party apparatus to prove its integrity and submitting the challenge to the entrusted computing apparatus" as recited by claim 12, the Applicants and the undersigned are mystified as to why this claim is being rejected based upon Ginter.

Claim 12 also recites "the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user." The Examiner cites column 19, lines 29-58 of Ginter as meeting this limitation. The passage cited by the Examiner includes a rather confusing discussion of how an electronic agreement can apparently be entered between parties. What this has to do with the discussion of the pattern matching engine 524 at column 68 just discussed above is unknown. Where is the nexus? Since there is no disclosure of the "trusted computing apparatus receiving the challenge" much less "the trusted device generating a response including the integrity metric and returning the response to the user" in the passage cited by the Examiner, the rejection of claim 12 under 35 USC 102 must fail.

Claim 12 also recites "the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated integrity metric for the trusted computing apparatus that had been generated by a trusted party." The Examiner cites column 9, lines 19-30 of Ginter as meeting this limitation. Why this passage which the Examiner refers to allegedly anticipates the just-quoted limitation is simply unknown. Also, what the nexus is between this passage, the passage cited at column 19, lines 29-58 and the passage cited at column 68, lines 29-42, is also unknown. The passages seem to be absolutely disconnected from one another.

It is as if the Examiner has cited a dictionary against claim 12, pointing out that the Examiner can find each word of claim 12 in the dictionary, and therefore the dictionary anticipates the claim. If it were so easy, then each and every invention that has ever been made and probably every invention that could ever be made, has already been anticipated by a dictionary.

The rejection of claim 12 under 35 USC 102 as allegedly being fully anticipated by Ginter is improper and should be overturned by the Board of Appeals.

Claim 13

Claim 13 adds the limitation to claim 12 of "wherein the challenge includes a nonce, the response includes the integrity metric and the nonce, both digitally signed by the trusted device using a information security algorithm, and the user verifies the integrity metric and the nonce using a respective information security algorithm."

With respect to claim 13, the Examiner rejects this claim under 35 USC 102 and points the Applicant to column 45, lines 49-62 of Ginter.

Note that claim 13 requires that the challenge include a nonce. Where is that disclosed in Ginter? The passage cited by the Examiner is silent on that point. Claim 13 also recites that "the response includes the integrity metric and the nonce, both digitally signed by the trusted device." What does the discussion at the passage cited by the Examiner have anything to do with that or any other portion of claim 13?

The Examiner's rejection of claim 13 is improper and should be overturned.

Claim 14

Claim 14 adds the recitation "wherein the trusted device uses a private encryption key to sign the integrity metric and the nonce, and the user uses the respective public encryption key to verify the integrity metric and the nonce."

The Examiner is silent as to why that claim is rejected other than to assert that it is "similar" to claim 12. Of course, that is not a proper grounds for rejection under 35 U.S.C. 102 and therefore this grounds for rejection should be overturned by the Board of Appeals.

Claim 15

Claim 15 adds a limitation to claim 14 to the effect that "the response includes a certificate held by the trusted device, which certificate has been digitally signed by a trusted party...the certificate including the public encryption key of the trusted device and the user verifies the certificate using the public encryption key of the trusted party and uses the public encryption key from the certificate to verify the integrity metric and the nonce."

Again, the Examiner is silent as to why claim 15 is being rejected, other than to assert that it is similar to claim 12. Of course, it is not similar to claim 12, and the Examiner has not pointed out why each and every limitation of claim 15 can allegedly be found in Ginter. Moreover, merely being "similar" to another claim is not a proper basis for rejecting a claim under 35 USC 102.

The rejection is improper and the Examiner should be so advised.

Claim 16

Claim 16 can be found in the enclosure. It includes a number of elements, none of which has the Examiner bothered to show that they allegedly are anticipated by Ginter.

The Examiner's actions are improper and this rejection should be overturned.

Claim 17

Claim 17 can be found in the enclosure. It includes a number of elements, none of which has the Examiner bothered to show that they allegedly are anticipated by Ginter.

The Examiner's actions are improper and this rejection should be overturned.

Claim 22

Claim 22 is a claim that is similar, in some regards, to claim 1, but the trusted device limitation is spelled out in somewhat greater detail since the trusted device is defined as being "adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric" in this claim.

As to the integrity metric limitation, in the final rejection the Examiner again points to column 68, lines 29-42 which includes the only mention of the word "metric" (in its plural form) in Ginter. Of course, as outlined above, the discussion of the "metrics" at that point in Ginter has nothing at all to do with "an integrity metric that measures that the computing apparatus is operating as intended" as claimed.

For the "correctness determination" (to quote the Examiner) the Examiner points to column 64, lines 1-15 of Ginter. At that point, Ginter gets into a discussion of the functions which the SPU 500's may perform, including "authentication and/or error correction validation of information."

However, there is no suggestion here that this authentication or error correction validation of information has anything to do with the metrics discussed at column 68, and the metrics discussed at column 68, as indicated above, have nothing to do with the "integrity metric" of claim 22. Ginter may determine the correctness of something, but it is certainly not the "acquired value of the integrity metric" as specifically claimed by claim 22.

The rejection of claim 22 is improper for the reasons outlined out above and therefore the Examiner's rejection thereof under 35 U.S.C. 102 as allegedly being fully anticipated by Ginter should be overturned by this Board of Appeals.

Claim 23

Claim 23 adds a limitation to claim 22 indicating "wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus."

In the telephone call alluded to below with the Examiner, the undersigned had the opportunity to briefly discuss claim 45, which also adds a similar limitation as claim 23 with respect to the metric being a digest of all or part of the BIOS. The Examiner pointed the undersigned to column 240, line 16 of Ginter wherein the reference discusses "fingerprinting" of the apparatus. However, that fingerprinting appears to have nothing at all to do with the metric mentioned at column 68, which the Examiner is relying upon in rejecting the independent claims.

Indeed, instead of using the ROM BIOS as the signature, Ginter suggests inserting signature values into unused disc sectors (one that is marked bad even though it may viably store information) instead as being a more reliable technique.

Of course, obtaining a device signature is a different thing altogether compared to obtaining information as to whether or not the device has been compromised.

The rejection of claim 23 is improper and should be overturned by the Board of Appeals.

Claim 24

Claim 24 recites that "the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus."

In the official action, the Examiner does not advise why that claim is being rejected on prior art grounds, other than to assert that the claim is somehow similar to claim 22.

Since the rejection of claim 22 is improper and since this dependent claim adds still further limitations that are not taught by Ginter, the rejection is improper and should be overturned.

Claims 27 and 28

Claim 27 adds the limitation to claim 22 that the trusted device comprises " a device memory" and claim 28 adds to claim 27 the limitation that the trusted device comprises "a trusted device processor."

Given the Examiner's reliance upon element 524 as meeting the trusted device limitation, then these claims also serve to further differentiate the trusted device from the disclosure of Ginter.

As such, the rejection of these claims under 35 U.S.C. 102 should be overturned.

Claims 29 and 30

Each of these claims depend from claim 28 and add additional limitations with respect to the recited trusted device processor. Since the Examiner has not demonstrated how element 524 cited by the Examiner meets the trusted device processor limitation, it is not understood how the additional limitations added by these claims could possibly be met by that device.

Since the onus is on the Examiner to explain why these claims are fully anticipated by the prior art reference of Ginter, and since the Examiner has not done that, the rejections under 35 U.S.C. 102 should be properly overturned.

Claims 31 and 32

Claims 31 and 32 add limitations similar to limitations found in claim 8 discussed above. As indicated above, since during the telephone conversation with the Examiner wherein claim 8 was discussed the Examiner could not identify where either the "secret" (found in claim 31) or where the "private asymmetric encryption key" (found is claim 32) is disclosed by Ginter, the Applicant has no idea as to why these claims are being rejected based upon Ginter.

Since the Examiner has not met the standard for showing where each and every limitation of these claims can be found in the prior art reference, their rejections should properly be reversed by this Board of Appeals.

Claim 33

Claim 33 adds a limitation similar to claim 9 set forth above. As indicated above, the Examiner has not made an effort to show why the limitation added by this claim is anticipated by Ginter, and therefore the Examiner's rejection of the claim based upon Ginter should be overturned.

Claim 34

Claim 34 adds a limitation somewhat similar to claim 10, which includes, amongst other things, the fact that the trusted device processor is "arranged to generate a response to a received challenge."

In any event, as discussed above, when discussing the limitations of similar claim 10 with the Examiner, the Examiner could not or would not tell the undersigned where the limitations of that claim could be found in the prior art and hence also the limitations of this claim.

Since the Examiner has failed to demonstrate either to the applicants or to this Board of Appeals where each and every limitation of claim 34 is anticipated by Ginter, the rejection of claim 34 based upon Ginter under 35 U.S.C. 102 should properly be overturned.

Claim 35

Claim 35 is another independent claim. It can be found in the enclosure. Claim 35 recites, in a computing apparatus comprising an assembly "a plurality of functional components including a main memory and a main processor mounted on the assembly, each functional component being connected for communication with one or other functional components on the assembly, a trusted device being one of said functional components and adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric."

The Examiner has made no effort to show how claim 35, and in particular the limitation with respect to "a trusted device being one of said functional components and being adapted to acquire a value of an integrity metric that measures that the computing apparatus is functioning as intended and determining the correctness of the acquired value of the integrity metric" is anticipated by Ginter.

In rejecting this claim under 35 USC 102, the Examiner asserts that this claim is "similar" to claim 22. Of course, that is not an appropriate grounds for rejecting a claim under 35 U.S.C. 102.

Since the Examiner has not pointed out how the limitations of claim 35 are allegedly anticipated by the prior art, this grounds for rejection should be overturned by this Board of Appeals.

Claim 36

Claim 36 is another independent claim. It can be found in the enclosure. Claim 36 recites "a trusted device for use as a functional component in a computing apparatus, the trusted device being adapted for mounting on an assembly of the computing apparatus and being adapted for communication with other functional components of the computing apparatus, the trusted device being adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric."

This claim is rejected by the Examiner under 35 USC 102 as allegedly teaching a "similar apparatus" as claim 22.

As indicated above, the Examiner has not demonstrated that Ginter anticipates a trusted device "adapted to acquire a value of an integrity metric." Moreover, claim 36 is different from claim 22 (and claim 1) in that it also recites that the integrity metric "measures that the computing apparatus is operating as intended." The only metric to which the examiner refers the applicant is the "metrics" related to pattern recognition in Ginter. But those metrics do not measure "that the computing apparatus is operating as intended" as claimed by claim 36.

Since the Examiner has not demonstrated that all the limitations of claim 36 are anticipated by Ginter, this grounds for rejection should properly be overturned by this Board of Appeals.

Claims 38 and 39

Claim 38 adds the limitation to claim 36 that the trusted device comprises " a device memory" and claim 39 adds to claim 38 the limitation that the trusted device comprises "a trusted device processor."

Given the Examiner's reliance upon element 524 as meeting the trusted device limitation, then these claims also serve to further differentiate the trusted device from the disclosure of Ginter.

As such, the rejection of these claims under 35 U.S.C. 102 should be overturned.

Claims 40 and 41

Claims 40 and 41 add limitations similar to limitations found in claim 8 and also found in claims 1 and 32, all discussed above. As indicated above, since during the telephone conversation with the Examiner wherein claim 8 was discussed the Examiner could not identify where either the "secret" (found in claim 40) or where the "private asymmetric encryption key" (found in claim 41) is disclosed by Ginter, the Applicant has no idea as to why claims 40 and 41 are being rejected based upon Ginter.

Since the Examiner has not met the standard for showing where each and every limitation of these claims can be found in Ginter, the rejections of claims 40 and 41 should properly be reversed by this Board of Appeals.

Claim 42

Claim 42 adds a limitation to claim 41 which is somewhat similar to claims 33 and 9 set forth above. As indicated above, the Examiner has not made an effort to show why the limitation added by this claim is anticipated by Ginter, and therefore the Examiner's rejection of the claim based upon Ginter should be overturned.

Claim 43

Claim 43 adds a limitation somewhat similar to claims 34 and 10, which recites, amongst other limitations, the fact that the trusted device processor is "arranged to generate a response to a received challenge."

As discussed above, when discussing the limitations of similar claim 10 with the Examiner, the Examiner could not or would not tell the undersigned where the limitations of that claim could be found in Ginter and hence it seems that the Examiner is similarly unwilling or unable to show where the limitations of this claim are allegedly anticipated by Ginter. It is not known how Ginter allegedly anticipates the limitation "arranged to generate a response to a received challenge" recited above.

Claim 43 also recites that "the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party", "the trusted device is adapted to employ an encryption function," "the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key." Where these elements can allegedly be found in Ginter is simply unknown to Applicants.

Since the Examiner has failed to demonstrate either to the applicants or to this Board of Appeals where each and every limitation of claim 43 is anticipated by Ginter, the rejection of claim 43 based upon Ginter under 35 U.S.C. 102 should properly be overturned.

Claim 44

Claim 44 adds a limitation to claim 1 that "the trusted device includes non-volatile memory for storing instructions instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means."

Claim 44 is rejected under 35 USC 102 for teaching a "similar apparatus" as claim 1. That is not a proper grounds for rejection.

Looking at the final rejection, the Examiner apparently points to element 524 as meeting the "trusted device" limitation of claim 1. But if that is the case, where is there any teaching of "non-volatile memory" in element 534, much less "non-volatile memory for storing instructions

instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means" as claimed?

In the aforementioned telephone call with the Examiner, the Examiner pointed to the fingerprinting described at column 240, line 16, of Ginter as already discussed above with reference to claim 23. However, that fingerprinting appears to have nothing at all to do with the metric mentioned at column 68, which the Examiner is relying upon in rejecting the independent claims.

Moreover, instead of using the ROM BIOS as the signature, Ginter suggests inserting signature values into unused disc sectors (one that is marked bad even though it may viably store information) for device signatures.

Of course, obtaining a device signature is a completely different thing than obtaining information as to whether or not the device has been compromised.

The rejection of claim 23 is improper and should be overturned by the Board of Appeals.

Claim 45

Claim 45 adds a limitation to claim 1 that "the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus."

Claim 45 is rejected under 35 USC 102 for teaching a "similar apparatus" as claim 1. That is not proper grounds for rejecting claim 45.

In the final rejection, the Examiner apparently points to element 524 as meeting the "trusted device" limitation of claim 1 and hence also of claim 45. But if that is the case, where is there any teaching of "a digest of all or part of the basic input/output software for the computing apparatus" as claimed in device 524?

In the aforementioned telephone call with the Examiner, the Examiner pointed to the fingerprinting described at column 240, line 16, of Ginter as already discussed above with reference to claims 23 and 44.

The final rejection of claim 45 is improper and should properly be overturned by this Board of Appeals.

Claim 46

Claim 46 adds a limitation to claim 1 somewhat akin to claim 45, but narrower in that "the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus."

Claim 46 is rejected under 35 USC 102 for teaching a "similar apparatus" as claim 1. That is not a proper grounds for rejection.

Claim 46 is not anticipated by either the passage at column 68 cited in the final rejection or by the passage at column 240 mentioned in the telephone call with the undersigned.

The final rejection of claim 46 is improper and should properly be overturned by this Board of Appeals.

Claim 49

Claim 49 adds a limitation to claim 1 reciting that "the trusted device is accessed by said main processing means prior to said main processing means accessing basic input/output software instructions stored in non-volatile memory during a boot process of said computing apparatus." Since the Examiner points to element 524 in the final rejection as meeting the "trusted device" limitation, then what element in Ginter is the recited "main processing means"?

Perhaps SPU 500? If that is the case, how is the pattern matching engine 524 "accessed by said main processing means" as specifically recited in this claim? On the other hand if the Examiner switches horses and instead points to SPU 500 as meeting the "trusted device" then what element or elements meet the "main processing means" limitation of claim 1 or the limitation of claim 49 that "the trusted device is accessed by said main processing means prior to said main processing means accessing basic input/output software instructions stored in non-volatile memory during a boot process of said computing apparatus"? Where is there any disclosure of any such accessing of instructions in Ginter? There is plenty of VDE code in Ginter, but what about the claimed instructions? Since the Examiner has not pointed to anticipatory instructions, the rejection of claim 49 must fail.

Claim 50

Claim 50 adds a limitation to claim 12 reciting that "the trusted device acquires the true value of the integrity metric of the trusted computing apparatus before a boot up process of the trusted computing apparatus is completed.

Claim 50 is rejected for teaching a "similar method" to claim 12. That is not a proper ground for rejecting a claim under 35 USC 102.

The Examiner is apparently relying on the passage at column 68 of Ginter to reject claim 50. To the extent that Ginter teaches a "metric", where is there any teaching that the metric is acquired "before a boot up process of the trusted computing apparatus is completed"? The Examiner fails to point out where Ginter allegedly meets this limitation.

Since the Examiner has not provided a proper statutory basis for rejecting this claim under 35 USC 102, the rejection should be properly overturned.

Claim 51

Claim 51 adds a limitation to claim 35 reciting that "the trusted device is adapted to acquire the value of the integrity metric before the computing apparatus has completed a boot up process."

Claim 51 is rejected for teaching a "similar apparatus" to claim 22. That is not a proper basis for rejecting a claim under 35 USC 102.

The Examiner is apparently relying on the passage at column 68 of Ginter to reject claim 51. To the extent that Ginter teaches a "metric", where is there any teaching that the metric is acquired "before the computing apparatus has completed a boot up process"? The Examiner fails to point out where Ginter allegedly meets this limitation.

Since the Examiner has not provided a proper statutory basis for rejecting this claim under 35 U.S.C. 102, the rejection of claim 51 should be properly overturned.

Claim 52

Claim 52 adds a limitation to claim 35 reciting "further including means for testing to assure that the trusted device is accessed by said main processor before said main processor accesses basic input/output instructions for booting the computing apparatus."

Claim 52 is rejected for teaching a "similar apparatus" to claim 22. That is not a proper basis for rejecting a claim under 35 USC 102.

The Examiner is apparently relying on the passage at column 68 of Ginter to reject claim 52. To the extent that Ginter teaches a "metric", where is there any teaching that the metric is acquired and means are provided "for testing to assure that the trusted device is accessed by said main processor before said main processor accesses basic input/output instructions for booting the

computing apparatus"? The Examiner fails to point out where Ginter allegedly meets this limitation.

Since the Examiner has not provided a proper statutory basis for rejecting this claim under 35 U.S.C. 102, the rejection of claim 52 should be properly overturned.

Claim 53

Claim 53 adds a limitation to claim 1 reciting that "said trusted device includes:

a. a measurement function for acquiring the integrity metric of the computing apparatus;
b. an authentication function for authenticating a user's smart card; and
c. a controller for interacting with the main processing means and the measurement and authentication functions."

The Examiner's rationale for rejecting this claim is based on the simple fact that Ginter "teaches the functions and activities of smart cards at least in col 8, lines 1-7 and col 100, lines 35-45."

Since the Examiner refers the applicant and the Board to column 68 as allegedly meeting the "integrity metric of the computing apparatus" limitation of claim 1, the element 524 disclosed thereat clearly has no disclosed "authentication function for authenticating a user's smart card" as claimed even if Ginter's electronic commerce solution can somehow utilize smart cards as noted by the Examiner. How does Ginter teach one to use smart cards? Ginter reads more like a press release than a technical disclosure of how to take advantage of smart cards and therefore it is not an enabling reference.

The Examiner has not provided a proper statutory basis for rejecting claim 53 under 35 USC 102, therefore the rejection of claim 53 should be properly overturned.

Claim 54

Claim 54 adds a limitation to claim 53 reciting that "said measurement function has access to memory in said trusted device for storing a private key of the trusted device and the integrity metric, the integrity metric indicating whether or not the trusted device was accessed by the main processor before said main processor accesses basic input/output instructions for booting the computing apparatus."

The Examiner's rationale for rejecting this claim is the same as for claim 53 quoted above. Since the Examiner has not provided a proper statutory basis for rejecting claim 53 under 35 U.S.C. 102, the rejection of claim 54 should also be properly overturned.

Additionally, either if one assumes the fact that Ginter allegedly "teaches the functions and activities of smart cards" as asserted by the Examiner in the final rejection, that does not justify this rejection under 35 USC 102. The Examiner ignores the language of claims 53 and 54.

The US patent law is very clear: a rejection under 35 USC 102 is improper if it fails to show where each and every limitation of the rejected claim can be found, expressly or inherently, in the prior art. The rejection of this claim utterly fails to meet this test and therefore the rejection should properly be overturned.

Issue 2: Is claim 54 sufficiently clear to avoid an objection by the Examiner?

The examiner objects to the term "private key" in claim 53 asserting that the term is "unclear to what it means within specification" [sic].

Both the terms "public key" and "private key" can be found in the specification. See, for example, page 7, lines 19 and 34. It is submitted that a person skilled in the computer security arts will be rather familiar with public-key encryption, a cryptographic system which uses two keys, a public key and a private key, as a means for safeguarding messages. A very famous

implementation of public key encryption is Pretty Good Privacy or PGP. It is submitted that persons skilled in this general area of technology will be familiar with PGP and its private and public keys.

There is nothing unclear in claim 54 by the use of the phase "private key" and the Examiner should be so advised by this Board of Appeals.

Issue 3: Is a rejection under 35 USC 102 proper just because a claim is allegedly similar to another claim in the same patent application?

Many claims in this application are finally rejected merely because the Examiner alleges that the claims either "teach a similar apparatus" or "teach a similar method" as other rejected claims. See the rejections of claims 2-10, 14-17, and 23-54.

The applicant has tried to obtain clarification of these matters before bringing this appeal. The applicant filed one RCE in hopes of clarifying matters, but that did not help. If the Board of Appeals compares the final rejection appealed from with the earlier final rejection dated March 19, 2004, the Board will see that the latest final rejection nearly parrots the earlier final rejection in providing scant reasons for rejecting the claims in this application. Trying to conduct an interview with the Examiner to clarify these matters before bringing this appeal also did not meet with success in terms of clarifying the grounds for rejecting the claims.

Issue 4: What is the Applicants' remedy when the Examiner violates the Rules of Practice?

Unfortunately, the only real remedy for Applicants is an appeal if the Examiner and his or her supervisor do not have the desire or inclination to follow the rules of practice. Undoubtedly, there should be a better way of handling these issues. Filing a petition to the Director should not be required, especially since the application could become abandoned while a petition was pending before the Director. The rules of practice set up remedies if applicants and/or their attorneys do not toe the line in following the rules, but the rules seem only to assume that Examiners will comply with the rules since no remedies are given to applicants if Examiners fail

to follow the rules of practice. The rules need to be overhauled so that Examiners are held to a higher standard of practice than which occurred during the examination of this application.

Conclusion

For the extensive reasons advanced above, Appellant respectfully contends that the rejection of each claim is improper. Therefore, reversal of all rejections is respectfully requested.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Office with sufficient postage as express mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22323-1450 on

May 18, 2005
(Date of Mailing)

Corinda Humphrey
(Name of Person Mailing)

Corinda Humphrey
(Signature)

May 18, 2005
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300

1. Computing apparatus ~~comprising~~, mounted on an assembly, main processing means, main memory means and a trusted device, each being connected for communication with one or more other components on the assembly,

the trusted device being arranged to acquire a true value of an integrity metric of the computing apparatus.

2. Computing apparatus according to claim 1, wherein the trusted device comprises device memory means and means for instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means.

3. Computing apparatus according to claim 2, wherein the means for instructing the main processing means comprises, stored in the device memory means, program code native to the main processing means, and the trusted device is arranged to transfer the instructions of the program code to the main processing means.

4. Computing apparatus according to claim 3, wherein the computing apparatus is arranged to cause the instructions to be the first instructions executed after release from reset.

5. Computing apparatus according to claim 3, wherein the trusted device is arranged to transfer the instructions to the main processing means in response to memory read signals from the main processing means.

6. Computing apparatus according to claim 1, wherein the trusted device comprises device memory means and is arranged to monitor a data bus means by which components mounted on the assembly are adapted to communicate and store in the device memory means a flag in the event the first memory read signals generated by the main processing means after the computing apparatus is released from reset are addressed to the trusted device.

7. Computing apparatus according to claim 1, wherein the trusted device has stored in device memory means at least one of:

a unique identity of the trusted device;

an authenticated integrity metric generated by a trusted party; and

a secret.

8. Computing apparatus according to claim 7, wherein the trusted device has stored in device memory means a secret comprising a private asymmetric encryption key.

9. Computing apparatus according to claim 8, wherein the trusted device also has stored in device memory means a respective public encryption key that has been signed by a trusted party.

10. Computing apparatus according to claim 8, wherein the trusted device has stored in device memory means an authenticated integrity metric generated by a trusted party and includes a encryption function, the trusted device being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

12. A method of operating a system comprising a trusted computing apparatus and a user, the trusted computing apparatus incorporating a trusted device being arranged to acquire the true value of an integrity metric of the trusted computing apparatus, the method comprising the steps of:

the trusted device acquiring the true value of the integrity metric of the trusted computing apparatus;

the user generating a challenge for the trusted computing apparatus to prove its integrity and submitting the challenge to the trusted computing apparatus;

the trusted computing apparatus receiving the challenge, and the trusted device generating a response including the integrity metric and returning the response to the user; and

the user receiving the response, extracting the integrity metric from the response and comparing the integrity metric with an authenticated metric for the trusted computing apparatus that had been generated by a trusted party.

13. A method according to claim 12, wherein the challenge includes a nonce, the response includes the integrity metric and the nonce, both digitally signed by the trusted device using a

information security algorithm, and the user verifies the integrity metric and the nonce using a respective information security algorithm.

14. A method according to claim 13, wherein the trusted device uses a private encryption key to sign the integrity metric and the nonce, and the user uses the respective public encryption key to verify the integrity metric and the nonce.

15. A method according to claim 14, wherein the response includes a certificate held by the trusted device, which certificate has been digitally signed by a trusted party using a private encryption key of the trusted party, the certificate including the public encryption key of the trusted device, and the user verifies the certificate using the public encryption key of the trusted party and uses the public encryption key from the certificate to verify the integrity metric and the nonce.

16. A method of establishing a communications channel in a system between trusted computing apparatus and remote computing apparatus, the method including the step of the remote computing apparatus verifying the integrity of the trusted computing apparatus using the method according to claim 12, and maintaining the communications channel for further transactions in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

17. A method of verifying that trusted computing apparatus is trustworthy for use by a user for processing a particular application, the method including the step of the user verifying the integrity of the trusted computing apparatus using the method according to claim 12, and the user using the trusted computing apparatus to process the particular application in the event the integrity of the trusted computing apparatus is successfully verified by the remote computing apparatus.

22. Computing apparatus comprising an assembly; a main processor, a main memory and a trusted device, each being mounted on the assembly and connected for communication with other components mounted on the assembly, wherein the trusted device is adapted to acquire a

value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

23. Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus.

24 .Computing apparatus as claimed in claim 22, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus.

25. Computing apparatus as claimed in claim 22, wherein the trusted device is adapted to acquire a plurality of integrity metrics.

26. Computing apparatus as claimed in claim 22, wherein the trusted device is adapted to be tamper resistant.

27. Computing apparatus as claimed in claim 22, wherein the trusted device comprises a device memory.

28. Computing apparatus as claimed in claim 27, wherein the trusted device comprises a trusted device processor.

29. Computing device as claimed in claim 28, wherein the trusted device processor is adapted to instruct the main processor to determine the integrity metric and return the integrity metric for storage in the device memory.

30. Computing apparatus as claimed in claim 28, wherein the trusted device processor is adapted to obtain information necessary to calculate the integrity metric and to calculate the integrity metric for storage in the device memory.

31. Computing apparatus as claimed in claim 28, wherein the trusted device has a secret stored in the device memory.

32. Computing apparatus as claimed in claim 31, wherein the secret comprises a private asymmetric encryption key.

33. Computing apparatus as claimed in claim 32, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

34. Computing apparatus as claimed in claim 33, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

35. In a computing apparatus comprising an assembly, a plurality of functional components including a main memory and a main processor mounted on the assembly, each functional component being connected for communication with one or more other functional components on the assembly, a trusted device being one of said functional components and adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

36. A trusted device for use as a functional component in a computing apparatus, the trusted device being adapted for mounting on an assembly of the computing apparatus and being adapted for communication with other functional components of the computing apparatus, the trusted device being adapted to acquire a value of an integrity metric that measures that the computing apparatus is operating as intended and determining the correctness of the acquired value of the integrity metric.

37. Computing apparatus as claimed in claim 36, wherein the trusted device is adapted to be tamper resistant.

38. Computing apparatus as claimed in claim 36, wherein the trusted device comprises a device memory.

39. Computing apparatus as claimed in claim 38, wherein the trusted device comprises a trusted device processor.

40. Computing apparatus as claimed in claim 39, wherein the trusted device has a secret stored in the device memory.

41. Computing apparatus as claimed in claim 40, wherein the secret comprises a private asymmetric encryption key.

42. Computing apparatus as claimed in claim 41, wherein the trusted device also has stored in the device memory in the device memory a respective public encryption key that has been signed by a trusted third party.

43. Computing apparatus as claimed in claim 42, wherein the trusted device also has stored in the device memory an authenticated integrity metric generated by a trusted third party and wherein the trusted device is adapted to employ an encryption function, the trusted device processor being arranged to generate a response to a received challenge, the response comprising an acquired integrity metric and the authenticated integrity metric, both signed by the encryption function using the private asymmetric encryption key.

44. Computing apparatus as claimed in claim 1, wherein the trusted device includes non-volatile memory for storing instructions instructing the main processing means to determine the integrity metric and return the integrity metric for storage in the device memory means.

45. Computing apparatus as claimed in claim 1, wherein the integrity metric is a digest of all or part of the basic input/output software for the computing apparatus.

46. Computing apparatus as claimed in claim 1, wherein the integrity metric is a digest of all or part of the basic input/output software for components or apparatus attached to the computing apparatus.

47. Computing apparatus as claimed in claim 1, wherein the trusted device is implemented as an application specific integrated circuit device.

48. Computing apparatus as claimed in claim 1, wherein the trusted device is implemented as a programmed micro-controller.

49. Computing apparatus as claimed in claim 1, wherein the trusted device is accessed by said main processing means prior to said main processing means accessing basic input/output software instructions stored in non-volatile memory during a boot process of said computing apparatus.

50. A method according to claim 12, wherein the trusted device acquires the true value of the integrity metric of the trusted computing apparatus before a boot up process of the trusted computing apparatus is completed.

51. The combination of claim 35 wherein the trusted device is adapted to acquire the value of the integrity metric before the computing apparatus has completed a boot up process.

52. The combination of claim 35 further including means for testing to assure that the trusted device is accessed by said main processor before said main processor accesses basic input/output instructions for booting the computing apparatus.

53. Computing apparatus as claimed in claim 1 wherein said trusted device includes:

d. a measurement function for acquiring the integrity metric of the computing apparatus;

e. an authentication function for authenticating a user's smart card; and

f. a controller for interacting with the main processing means and the measurement and authentication functions.

54. Computing apparatus as claimed in claim 53 wherein said measurement function has access to memory in said trusted device for storing a private key of the trusted device and the integrity metric, the integrity metric indicating whether or not the trusted device was accessed by the main processor before said main processor accesses basic input/output instructions for booting the computing apparatus.